Available online at www.sciencedirect.com
ScienceDirect
Discrete Applied Mathematics 156 (2008) 3150–3154
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

On RSA moduli with almost half of the bits prescribed

Sidney W. Graham[a], Igor E. Shparlinski[b,*]

[a] *Department of Mathematics, Central Michigan University, Mount Pleasant, MI 48859, USA*
[b] *Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*

Received 1 March 2007; received in revised form 18 September 2007; accepted 19 December 2007
Available online 6 March 2008

Abstract

We show that using character sum estimates due to H. Iwaniec leads to an improvement of recent results about the distribution and finding RSA moduli $M = pl$, where p and l are primes, with prescribed bit patterns. We are now able to specify about n bits instead of about $n/2$ bits as in the previous work. We also show that the same result of H. Iwaniec can be used to obtain an unconditional version of a combinatorial result of W. de Launey and D. Gordon that was originally derived under the Extended Riemann Hypothesis.

Keywords: RSA; Bit pattern; Sparse integer; Smooth integer; Character sum; Hadamard matrices

1. Introduction

For an integer n, we use $\mathcal{P}_n$ to denote the set of primes p with $2^{n-1} < p < 2^n$. Let $\mathcal{M}_n$ be the set of RSA moduli $M = p\ell$ that are products of two distinct primes $p, \ell \in \mathcal{P}_n$.

Thus each $M \in \mathcal{M}_n$ has either $2n - 1$ or $2n$ bits which we number from the right to the left.

Motivated by some cryptographic applications (in particular by the idea of reducing the size of the public key), various heuristic algorithms have been given to construct moduli $M \in \mathcal{M}_n$ having a sufficiently long specified bit pattern have been given in [7,11]. Unfortunately, giving a rigorous analysis of these algorithms requires a very strong form of *Linnik's Theorem*, which far exceeds our current state of knowledge.

A different algorithm was proposed in [10]. Certainly this algorithm is likely to produce moduli having shorter prescribed bit patterns than those of [7,11]. However, using exponential sums, this algorithm has been rigorously analysed and shown the output in expected polynomial time a desired modulus $M \in \mathcal{M}_n$ with about $n/2$ prescribed bits.

Here we use the bound of character sums of Iwaniec [5] (see also [2,3] and the references therein) instead of bounds on exponential sums. This allows us to show that in fact the same algorithm can be used to generate in expected polynomial time a desired RSA modulus $M \in \mathcal{M}_n$ with about n prescribed bits.

* Corresponding author.
E-mail addresses: sidney.w.graham@cmich.edu (S.W. Graham), igor@ics.mq.edu.au (I.E. Shparlinski).

0166-218X/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2007.12.012

Our result immediately yields an improvement of Theorem 5 in [10], producing RSA moduli $M \in \mathcal{M}_n$ with at least $(3/2 + o(1))n$ zero bits. As in [10] we remark that such moduli may be useful for the *Paillier cryptosystem*, see [9], where one computes Mth powers.

We also outline some possible applications of the same ideas to generating sparse RSA moduli and smooth numbers (that is, numbers free of large prime factors) with a prescribed bit pattern, hence improving some other results of [10].

We end up with an observation that the results of [5] can also be used to eliminate the assumption of the Extended Riemann Hypothesis from a result of de Launey and Gordon [1].

Throughout the paper, $\mathcal{P}$ denotes the set of primes and $\ln z$ denotes the natural logarithm of $z > 0$.

2. RSA moduli with prescribed bit patterns

We recall the algorithm of [10] to generate an RSA modulus M having a desired bit pattern on certain positions.

Given a binary string σ of length m, we denote by $\mathcal{M}_{n,m}(\sigma)$ the set consisting of $M \in \mathcal{M}_n$ such that the bits of M at the positions $n-1, \ldots, n-m$ form the binary string σ.

Algorithm RSA-Modulus (n, m, σ)

Step 1 Choose an odd integer k in the interval $1 \le k < 2^{n-m}$ and a prime $p \in \mathcal{P}_n$ uniformly at random.

Step 2 Compute the positive integer $r < 2^n$ which satisfies the congruence

$$pr \equiv 2^{n-m}s + k \pmod{2^n},$$

where s is the integer whose binary representation coincides with σ.

Step 3 Test whether $2^{n-1} < r$, $r \ne p$ and also test r for primality, if r is prime then put $l = r$ and output $M = pl$, otherwise go to Step 1 and start a new round of the algorithm.

Certainly, if Algorithm RSA-MODULUS (n, m, σ) terminates it outputs $M \in \mathcal{M}_{n,m}(\sigma)$.

Theorem 1. *For $m = \lfloor n - n^{3/4} \ln n \rfloor$ and any binary string σ of length m, Algorithm* RSA-MODULUS (n, m, σ) *terminates in expected polynomial time.*

Proof. As in [10], for an integer $0 \le k \le 2^{n-m} - 1$, we denote by $N(k)$ the number of solutions $p, l \in \mathcal{P}_n$ to the congruence $pl \equiv 2^{n-m}s + k \pmod{2^n}$ where binary representation of the integer s is given by the string σ (certainly $N(k) = 0$ for every even k).

Let $\mathcal{X}$ be the set of multiplicative characters modulo 2^n (see [6, Chapter 3] for a background on characters and character sums).

We also use $\mathcal{X}^*$ to denote the set of nonprincipal characters. We recall the orthogonality relation

$$\sum_{\chi \in \mathcal{X}} \chi(u) = \begin{cases} 0, & \text{if } u \not\equiv 1 \pmod{2^n}, \\ 2^{n-1}, & \text{if } u \equiv 1 \pmod{2^n}, \end{cases} \tag{1}$$

see [6, Section 3.2].

By (1), we have

$$N(k) = \frac{1}{2^{n-1}} \sum_{p,\ell \in \mathcal{P}_n} \sum_{\chi \in \mathcal{X}} \chi((2^{n-m}s - k)p^{-1}\ell^{-1}),$$

where the inverse values p^{-1} and ℓ^{-1} are taken modulo 2^n.

Changing the order of summation and separating the term $(\#\mathcal{P}_n)^2 2^{-n+1}$ corresponding to the principal character we obtain

$$\begin{aligned} N(k) &= (\#\mathcal{P}_n)^2 2^{-n+1} + \frac{1}{2^{n-1}} \sum_{\chi \in \mathcal{X}^*} \chi\left(2^{n-m}s + k\right) \sum_{p,l \in \mathcal{P}_n} \chi\left(p^{-1}\ell^{-1}\right) \\ &= (\#\mathcal{P}_n)^2 2^{-n+1} + \frac{1}{2^{n-1}} \sum_{\chi \in \mathcal{X}^*} \chi\left(2^{n-m}s + k\right) \left(\sum_{p \in \mathcal{P}_n} \chi\left(p^{-1}\right) \right)^2. \end{aligned}$$

Therefore

$$\sum_{k=0}^{2^{n-m}-1} N(k) = \frac{(\#\mathcal{P}_n)^2}{2^m} + \Delta, \tag{2}$$

where

$$\Delta = \frac{1}{2^{n-1}} \sum_{\chi \in \mathcal{X}^*} \sum_{k=0}^{2^{n-m}-1} \chi\left(2^{n-m}s + k\right) \left(\sum_{p \in \mathcal{P}_n} \chi\left(p^{-1}\right) \right)^2.$$

Using the triangle inequality, we conclude that

$$\begin{aligned} |\Delta| &= \frac{1}{2^{n-1}} \left| \sum_{\chi \in \mathcal{X}^*} \sum_{k=0}^{2^{n-m}-1} \chi\left(2^{n-m}s + k\right) \left(\sum_{p \in \mathcal{P}_n} \chi\left(p^{-1}\right) \right)^2 \right| \\ &\le \frac{1}{2^{n-1}} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{k=0}^{2^{n-m}-1} \chi\left(2^{n-m}s + k\right) \right| \left| \sum_{p \in \mathcal{P}_n} \chi\left(p^{-1}\right) \right|^2 \\ &= \frac{1}{2^{n-1}} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{k=0}^{2^{n-m}-1} \chi\left(2^{n-m}s + k\right) \right| \left| \sum_{p \in \mathcal{P}_n} \chi\left(p\right) \right|^2, \end{aligned}$$

since the values of $\chi(p)$ and $\chi\left(p^{-1}\right)$ are conjugated over $\mathbb{C}$.

We now recall that by [5, Lemma 6],

$$\sum_{k=0}^{2^{n-m}-1} \chi\left(2^{n-m}s + k\right) \ll 2^{n-m} n^{-2}$$

provided that

$$2^{n-m} \gg 2^{n^{3/4} \ln n},$$

which is satisfied for our choice of m.

Therefore

$$\begin{aligned} |\Delta| &\ll \frac{1}{2^m n^2} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{p \in \mathcal{P}_n} \chi\left(p\right) \right|^2 \le \frac{1}{2^m n^2} \sum_{\chi \in \mathcal{X}} \left| \sum_{p \in \mathcal{P}_n} \chi\left(p\right) \right|^2 \\ &= \frac{1}{2^m n^2} \sum_{p, \ell \in \mathcal{P}_n} \sum_{\chi \in \mathcal{X}} \chi\left(p\ell^{-1}\right). \end{aligned}$$

By (1) we see that inner sum vanishes unless $p \equiv \ell \pmod{2^n}$, which is equivalent to $p = \ell$. Therefore

$$|\Delta| \ll \frac{2^{n-m} \#\mathcal{P}_n}{n^2}. \tag{3}$$

Since $\#\mathcal{P}_n \gg 2^n n^{-1}$, substituting the bound (3) in (2) we derive

$$\sum_{k=0}^{2^{n-m}-1} N(k) = \left(1 + O(n^{-1})\right) \frac{(\#\mathcal{P}_n)^2}{2^m}.$$

This is a full analogue of the asymptotic formula (4) in [10] (except that the value of m is now different). Accordingly, the rest of the proof is identical to that of Theorem 4 in [10]. □

As we have remarked, Theorem 1 immediately yields the following improvement of Theorem 5 in [10] which can be have some application for the *Paillier cryptosystem* (see [9]).

Corollary 1. *For* $m = \lceil n - n^{3/4} \ln n \rceil$ *and the* m*-dimensional zero string* $\vartheta = (0, \ldots, 0)$ *of length* m*, Algorithm* RSA-MODULUS (n, m, ϑ) *terminates in expected polynomial time and with probability* $1 + o(1)$ *outputs a modulus* $M \in \mathcal{M}_n$ *with at most* $(1/2 + o(1))n$ *nonzero bits.*

3. Other applications

One can use a similar approach to improve Theorem 6 of [10] which guarantees the existence of certain smooth numbers with prescribed bit patterns.

Moreover, without any substantial changes, an analogue of Theorem 1 can be obtained for the values of the Euler function $\varphi(p\ell) = (p-1)(\ell-1)$. For example, one can prove that for any r, there are r-bit integers R such that the binary expansion of $\varphi(R)$ contains $(3/4 + o(1))r$ nonzero digits. This can be extended to g-ary expansions for any base g.

Finally, we conclude with noticing that the results of [3,5] have direct implications on the distribution of primes in arithmetic progressions modulo 2^n. P.X. Gallagher [3] proves that if $q = p^r$ (p odd) and if $q \cdot x^{3/5+\epsilon} \le h \le x$, then

$$\psi(x + h, q, a) - \psi(x, q, a) \sim \frac{h}{\varphi(q)} \tag{4}$$

whenever $(a, q) = 1$, where, as usual,

$$\psi(x, q, a) = \sum_{\substack{k \le x \\ k \equiv a \pmod q}} \Lambda(k)$$

and

$$\Lambda(k) = \begin{cases} \log p & \text{if } k \text{ is a power of a prime } p, \\ 0 & \text{otherwise,} \end{cases}$$

is the von Mangoldt function, see [6, Chapter 5.9]. The exponent $3/5$ came from appealing to a zero-density estimate of Montgomery [8]. For technical reasons, Gallagher [3] excludes consideration of the case $p = 2$, but his proof can be easily modified to this case. The details of this modification (and much more) have been given by Iwaniec [5]. By using a zero-density result of Huxley [4] in conjunction with [5], one sees that (4) is true with $q = 2^r$ and $q \cdot x^{7/12+\epsilon} \le h \le x$. This result can be used in place of the Extended Riemann Hypothesis in the paper of de Launey and Gordon [1]. In particular, in the last undisplayed equation on page 184 of [1], one may take $y = \lfloor n^{7/12+\epsilon} \rfloor$. In turn, this yields an unconditional version of Theorem 1.2 of [1], albeit with a weaker error term:

$$r(N) \ge \frac{N}{2} + O(N^{113/132+o(1)})$$

for any $N \equiv 0 \pmod 4$, where $r(N)$ is the largest R for which there is an $R \times N$ Hadamard matrix (that is, ± 1 matrix H with $HH^T = NI_R$, where I_R is the $R \times R$ identity matrix). The exponent $113/132$ arises as

$$\frac{\alpha}{1+\alpha} + \frac{7}{12} = \frac{113}{132},$$

where, as in [1], we take $\alpha = 3/8$. In the conditional result of de Launey and Gordon [1], the $7/12$ term is replaced by $1/2$, thus giving the exponent

$$\frac{7}{22} = \frac{113}{132} - \frac{1}{12}.$$

References

[1] W. de Launey, D. Gordon, A comment on the Hadamard conjecture, J. Combin. Theory Ser. A 95 (2001) 180–184.

[2] A. Fujii, P.X. Gallagher, H.L. Montgomery, Some hybrid bounds for character sums and Dirichlet L-functions, in: Topics in Number Theory, in: Colloq. Math. Soc. Janos Bolyai, vol. 13, North-Holland, Amsterdam, 1976, pp. 41–57.

[3] P.X. Gallagher, Primes in progressions to prime-power modulus, Invent. Math. 16 (1972) 191–201.
[4] M.N. Huxley, Large values of Dirichlet polynomials. III, Acta Arith. 26 (1974–75) 435–444.
[5] H. Iwaniec, On zeros of Dirichlet's L series, Invent. Math. 23 (1974) 97–104.
[6] H. Iwaniec, E. Kowalski, Analytic Number Theory, in: AMS Colloquium Publications, vol. 53, Amer. Math. Soc., 2004.
[7] A.K. Lenstra, Generating RSA moduli with a predetermined portion, in: Lect. Notes in Comp. Sci., vol. 1514, Springer-Verlag, Berlin, 1998, pp. 1–10.
[8] H.L. Montgomery, Topics in Multiplicative Number Theory, in: Lecture Notes in Mathematics, vol. 227, Springer-Verlag, Berlin, 1971.
[9] P. Paillier, Public key cryptosystems based on composite degree residuosity classes, in: Lect. Notes in Comp. Sci., vol. 1592, Springer-Verlag, Berlin, 1999, pp. 223–238.
[10] I.E. Shparlinski, On RSA moduli with prescribed bit patterns, Designs, Codes Cryptogr. 39 (2006) 113–122.
[11] S.A. Vanstone, R.J. Zuccherato, Short RSA keys and their generation, J. Cryptology 8 (1995) 101–114.